

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **NORTHERN DISTRICT OF CALIFORNIA**
10 **SAN FRANCISCO DIVISION**

11 FACEBOOK, INC., a Delaware corporation,

12 Plaintiff,

13 v.

14 BRANDTOTAL LTD., an Israeli corporation,
15 and UNIMANIA, INC., a Delaware
16 corporation,

17 Defendants.
18
19
20
21
22
23
24
25
26
27
28

Case No. 3:20-CV-07182-JCS

**DECLARATION OF SANCHIT KARVE IN
SUPPORT OF PLAINTIFF'S OPPOSITION
TO DEFENDANTS' *EX PARTE* MOTION
FOR A TEMPORARY RESTRAINING
ORDER**

DECL. OF SANCHIT KARVE

1 I, Sanchit Karve, declare:

2 1. I submit this declaration in support of Plaintiff Facebook, Inc.'s ("Facebook")
3 Opposition in the above-captioned matter. I have personal knowledge of the facts set forth herein,
4 and if called to testify as a witness, I could do so competently under oath.

5 2. I have a Bachelor's and Master's degree in computer science. I have professional
6 experience in malware analysis, including reverse engineering malware.

7 3. I am employed by Facebook as a Malware Researcher on the eCrime team at
8 Facebook. I have been employed by Facebook since 2018. My responsibilities as a Malware
9 Researcher include identifying types of malware (*e.g.* ransomware, banking Trojan, keylogger, data
10 scraper), malware vulnerabilities (*e.g.* method used to obtain access to the targeted computer), the
11 infrastructure used by the malware (*e.g.* servers, IP addresses, domain names), and malware
12 functionality (*e.g.* steal login credentials, banking information). On the eCrime team, I also have
13 access to Facebook and Instagram account and administrative records.

14 **I. Unimania and BrandTotal Extensions and Apps**

15 4. In or around April 2020, I began investigating multiple browser extensions on the
16 Google Chrome Store believed to be scraping data from Facebook and Instagram.

17 5. Since April 2020, I have investigated and researched the activities of the following
18 browser extensions (a and b) and app (c) developed by or controlled by BrandTotal and Unimania:

- 19 a. UpVoice
- 20 b. Ads Feed
- 21 c. Anonymous Story Viewer for Instagram

22 6. I also reviewed a report published by the co-founder of AdGuard (attached as
23 Exhibit 1) that assessed the activities of the following browser extensions that AdGuard identified as
24 being used by Unimania to harvest data from Facebook:

- 25 a. Video Downloader for Facebook
- 26 b. Album & Photo Manager for Facebook
- 27 c. PDF Merger – PDF Files Merger
- 28 d. Pixcam – Webcam Effects

1 7. The UpVoice and Ads Feed and the extensions identified in paragraph 6 were
2 available for download through the Google Chrome Store. As of October 18, 2020, the Anonymous
3 Story Viewer for Instagram app was available for download from the Google Play store. I identified
4 multiple versions of the Ads Feed and UpVoice extensions from the Google Chrome Store. A new
5 version of an extension usually means something in the code of the extension was changed.

6 8. Internet browsers, such as Google Chrome, Opera, and Mozilla Firefox, are used to
7 access the internet. Internet browsers follow instructions from websites, in computer code, to render
8 and display a website's content for users to see. Website content is largely delivered in HTML code.
9 Internet browsers are designed to render the HTML code and display it in images and text for the
10 user's screen.

11 9. Internet browser extensions are software components that alter a browser's
12 functionality. Browser extensions can be installed to enhance user experience and the functionality
13 of the browser. For example, a browser extension can block pop-up ads.

14 10. Browser extensions can also be used in illicit ways. Browser extensions can be coded
15 to access the full array of information available to the browser and its functionalities. For example, a
16 browser extension can be designed to monitor a user's browsing session, manipulate how the content
17 of visited websites is displayed, and take other unauthorized actions.

18 11. A mobile app, like Anonymous Story Viewer for Instagram, is a computer program
19 designed to run on a mobile or tablet that provide the user with a function or service.

20 12. As a part of my investigation, I downloaded and reviewed the Ads Feed and UpVoice
21 extensions. Included in each download was a ZIP file that contained the extensions' JavaScript
22 source code. By reviewing that source code, I was able to understand how each extension worked
23 and the functionality of each extension. I also reviewed a technical analysis of the app --
24 Anonymous Story Viewer for Instagram - prepared by the Facebook External Data Misuse ("EDM")
25 team. EDM's technical analysis was prepared after downloading the app from the Google Play Store
26 and reviewing its code and testing the app.

27 13. The UpVoice and Ads Feed extensions and the Anonymous Story Viewer for
28 Instagram app are automated scraping tools. Once installed by a user, the extensions and app were

1 coded to automatically scrape information and data without the user having to do anything other than
2 visit the website targeted for scraping. To accomplish this, the extensions and app were coded to
3 exploit the legitimate user's browser as a proxy to access password-protected information on
4 Facebook and Instagram and request data while pretending to be an authenticated Facebook or
5 Instagram user with legitimate login credentials. This method of scraping allowed BrandTotal and
6 Unimania to access password-protected locations on Facebook's computers and obfuscate the
7 extensions' and app's activity from Facebook and Instagram.

8 **II. Information Scraped by BrandTotal and Unimania Extensions and App**

9 **A. UpVoice Browser Extension**

10 14. I reviewed multiple versions of the UpVoice extension that were available between
11 April 2020, and October 2020. On October 1, 2020 the UpVoice extension was removed from the
12 Google Chrome store. On October 12, 2020, I learned that a new extension named "UpVoice" was
13 publicly accessible on the Chrome Store. Exhibit 2. That version of the extension was removed
14 from the Chrome Store on or about October 14, 2020 and published again that same day. Exhibit 3.
15 It remained on the Google Chrome Store until on or about October 18, 2020. At the time it was
16 removed, information on the Chrome Store showed it had been downloaded at least 150 times.
17 Based on my analysis of the version of the UpVoice extension made available on October 12, 2020
18 (see Exhibit 2), that version of the extension was operational at that time and it exfiltrated data and
19 information from Facebook's computers.

20 15. Once a user installed the UpVoice extension, the extension used the user's browser as
21 a proxy to access Facebook computers and request data from Facebook while pretending to be an
22 authenticated Facebook user with legitimate login credentials. This method of scraping allowed
23 BrandTotal and Unimania to access password-protected areas on Facebook's computers and
24 obfuscates the extension's activity from Facebook.

25 16. With respect to the collection of Facebook data, each version of the UpVoice
26 extension that I reviewed was functionally identical. Each worked in a similar way and was coded to
27 scrape the same information from Facebook computers. Based on my review of the UpVoice
28

1 extension, I concluded it violates section 3.2.3 of the Facebook Terms of Service, which prohibits
2 accessing or collecting data using automated means without Facebook's permission.

3 17. To the best of my knowledge, each version of the UpVoice extension that I reviewed
4 scrapes, has scraped, or was coded to scrape the following information and data from Facebook's
5 computers when a user who had installed the extension visited the Facebook platform:

6 a. User profile information. The versions of the UpVoice extension that I
7 reviewed were coded to scrape data and information from users' Facebook profiles, including their
8 Facebook user IDs, gender, date of birth, self-disclosed location, and relationship status. A user's
9 Facebook ID is a unique identification number that is associated with that user's Facebook account.
10 Depending on the user's profile privacy settings, a user's date of birth, self-disclosed location, and
11 relationship status can be publicly viewable or private, but the versions of the UpVoice extension
12 that I reviewed were coded to scrape that information regardless of the user's privacy settings.
13 Additionally, I determined that the user profile information was scraped even if the user did not
14 access the profile settings where this information was located.

15 b. Advertising interests. Every Facebook user profile contains Ad Preference
16 information that includes the user's advertising interests by category. Ad Preference information is
17 not publicly viewable but is accessible to the authenticated Facebook user through their profile
18 settings. The versions of the UpVoice extension that I reviewed were coded to scrape user
19 advertising-interest categories from its non-publicly viewable location in user settings.

20 Categories of advertising interests can include, for example, "Parenting," "Home
21 Improvement," or "Shopping," but they can also be more specific. Facebook generates these
22 categories of interests based on a user's activities on Facebook. Clicking on advertisements for
23 children's products, for example, may result in the "Parenting" category being added to a user's list
24 of advertising interests. Users can access and opt-out of categories if they no longer wish to see
25 advertisements of that type. Facebook uses this information internally to determine what
26 advertisements to display to a particular user. Individual users can access information about their
27 own advertising interests while they are logged into their Facebook account. But the information
28 cannot be accessed by anyone other than the individual user and Facebook's internal systems.

1 c. Advertisements. The versions of the UpVoice extension that I reviewed were
2 coded to scrape information about advertisements viewed by users who had installed the extension,
3 including an advertisement's text, images or videos, buttons that users can click to navigate to other
4 webpages, and data on who sponsored the advertisements, all from a non-publicly viewable location
5 on Facebook. The versions of the UpVoice extension I reviewed were also coded to scrape the
6 Uniform Resource Locator or "URL" associated with every aspect of an advertisement and any "call
7 to action" buttons (e.g. "click here") that the advertisement contained. The URLs provided the
8 addresses to permanent webpages that contain the images used in the advertisements or the website
9 linked through the buttons on those advertisements. URLs for full advertisements from a user's New
10 Feed were only available to authenticated Facebook users. The URLs scraped by the UpVoice
11 extension enable users and non-users to view advertisements and advertising metrics (discussed below
12 in section II.A.(d)) even after the advertisement became inactive at the end of its campaign duration.

13 d. Advertising Metrics. Facebook users can engage with an advertisement in
14 various ways, including by commenting on it, sharing it, or reacting to it using Facebook's
15 prepopulated reactions—thumbs up, heart, a laughing face, a surprised face, a sad face, and an angry
16 face. Only authenticated users can comment, share, or react to an advertisement. For any
17 advertisement viewed by a Facebook user who installed the UpVoice extension, the UpVoice
18 extension scraped the number of comments, reactions, shares associated with the advertisement.
19 These advertising metrics are not publicly viewable in the Ads Library. These metrics are viewable
20 to other authenticated Facebook users on Facebook and non-users who have access to the
21 advertisement's URL scraped by the UpVoice extension.

22 e. Instagram. Certain versions of the UpVoice extension that I reviewed were
23 also coded to scrape data from Instagram. Those versions were coded to automatically scrape
24 certain data from Instagram when a user who installed the extension visited Instagram. The
25 extension was coded to scrape the Instagram user's name, account name, user ID, and profile picture
26 and, similar to the way it scraped data from Facebook, advertisements and advertising metrics. I
27 could not identify anything in the extension's code that anonymized the user profile information that
28 was scraped. The most recent version of the UpVoice extension did not scrape data from Instagram.

B. Ads Feed Browser Extension

18. I reviewed multiple versions of the Ads Feed extension. The Ads Feed extension was removed from the Google Chrome Store on October 1, 2020. Based on my review of the source code for the Ads Feed extension, I determined that all the versions of the extension I reviewed used code almost identical to the UpVoice extensions that I reviewed. The Ads Feed extensions I reviewed were also coded to scrape data from Instagram.

19. Like the UpVoice extensions that I reviewed, once a user installed the Ads Feed extension, the extension used the user's browser as a proxy to access Facebook computers and request data from Facebook while pretending to be an authenticated Facebook user with legitimate login credentials. This method of scraping allowed BrandTotal and Unimania to access password-protected areas on Facebook's computers and obfuscates the extension's activity from Facebook.

20. As to Facebook, the Ads Feed extension was coded to scrape the same user profile information, advertisements and advertising metrics, and Ad Preference information as the UpVoice extension. As to Instagram, the extension was coded to scrape the same information from Instagram as earlier versions of the UpVoice extension.

21. The data scraped by the Ads Feed extension was sent to the same servers as the data collected through the UpVoice malicious extension.

C. Anonymous Story Viewer for Instagram

22. In early October 2020, the Facebook EDM team downloaded and reviewed the Anonymous Story Viewer for Instagram app from the Google Play store. Unimania is listed as the developer of that app. Based on their analysis of the app, as of April 15, 2020, the app was scraping, from a user who installed the app and visited Instagram, the Instagram users ID, name of the user, phone number, email address, gender profile picture, Instagram accounts followed by the user and the name of the Instagram accounts following the user, the user's posts, and the comments and captions for posts, the URL for the posts, and the geotag of the Instagram post which is information embedded in the metadata of the photo that shows where the photo in the post was taken. None of the information was anonymized and was sent to a third-party server in plain text.

1 23. The app was also coded to scrape the session token and the user's session ID. This
2 information was exfiltrated to a third-party server as well. Anyone who possessed the session token
3 and session ID could make requests to Facebook computers for Instagram content for that user
4 without the user accessing Instagram.

5 **D. Ad Guard Report**

6 24. On May 30, 2018, AdGuard released a report analyzing what it identified to be four
7 browser extensions being used by Unimania to collect data. Exhibit 1. According to their website,
8 AdGuard is a software company focused on technology used to block ads on the internet. According
9 to the AdGuard report, the extensions they reviewed were coded to scrape data from Facebook
10 immediately after a user who installed one of the browser extensions opened their Internet browser.
11 Like the data scraped by the UpVoice and Ads Feed extensions, the data scraped by the extensions
12 discussed in the AdGuard report included data from a non-publicly viewable (*i.e.* password
13 protected) location on Facebook, and included a user's advertising interests, Facebook ID, and
14 advertisements.

15 25. According to the Ad Guard report, the extensions attempted to anonymize the user's
16 Facebook ID being scraped with a "static salt." The static salt replaced the user's Facebook ID—the
17 number associated with their Facebook profile—with a different set of unique numbers. Although
18 the Facebook user ID was no longer viewable as plain text, the static salt was a very weak form of
19 anonymization protection. It could be reversed very quickly, likely in under a minute, using publicly
20 available programs. The AdGuard published the instructions for reverse engineer the static salt used
21 by Unimania. Exhibit 1. By reverse engineering the static salt, anyone would have been able to
22 determine the Facebook ID number associated with the information scraped by those extensions.
23 The Facebook user ID could then be used to view the Facebook profile of the associated user and
24 connect the user to the information scraped by the extensions.

25 26. According the Ad Guard report, the data scraped through the extensions discussed in
26 the report was sent to the same servers as the data collected through the UpVoice and Ads Feed
27 extension that I reviewed. Policy statements in shown in the AdGuard report list Unimania as the
28 recipient of the data.

Facebook Accounts Associated with BrandTotal

27. I have viewed Facebook's and Instagram's user-account records for the accounts associated with Defendants.

28. Instagram account #####09355 ("Account 1") was created on December 6, 2016, uses the name "BrandTotal" and the username "brandtotal," and registration email address oren@brandtotal.io. Account 1 later changed their email address to social@brandtotal.io. Account 1 was disabled by Instagram on September 30, 2020.

29. Facebook account #####15996 ("Account 2") was created on June 13, 2017, uses the name "BrandTotal Analytics," and the registration email address social@brandtotal.io which is the same email address most recently used by Account 1. On June 13, 2017, Account 2 created Facebook Page #####52366 ("Page 1"), named it "BrandTotal," and used it to promote BrandTotal's marketing service. Page 1 and Account 2 were disabled by Facebook on September 30, 2020.

30. Facebook business account #####12689 ("Business 1") was created on February 21, 2017, using the name "BrandTotal." Page 1 was added as an asset to Business 1 giving it ownership on August 6, 2017. Business 1 owned one Facebook advertising account which promoted Page 1.

Accounts Associated With UpVoice

31. Facebook business account #####46916 ("Business 2") was created on September 3, 2019, using the name "UpVoice." Business 2 owned two Facebook advertising accounts which promoted Facebook Page #####68029 ("Page 2") named "UpVoice." Page 2, created January 24, 2019, was used to promote UpVoice's extensions and directed viewers to external website "joinupvoice.com." Business 1 owned two Facebook advertising accounts which promoted Page 2. Page 2 was disabled on September 30, 2020.

32. Facebook business account #####86182 ("Business 3") was created on June 8, 2020, using the name "UpVoice US." Page 2 was added as an asset to Business 3 giving it ownership on June 8, 2020. Business 3 owned one Facebook advertising account which promoted Page 2.

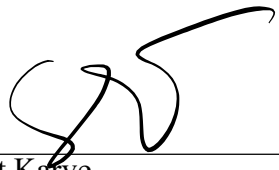
Accounts Associated With Unimania

33. Facebook business account #####61051 ("Business 4") was created on July 4, 2018, using the name "Unimania." Business 4 owned one Facebook advertising account which promoted Facebook Page #####47488 ("Page 3"). Page 3 was created on July 30, 2018, using the name "Ads Feed," was added as an asset to Business 4 on July 30, 2018, and was used to promote Unimania's extension. Page 3 was disabled on September 30, 2020.

New Facebook and Instagram Accounts

34. On October 3, 2020, Facebook account #####68025 was created using the name "Jack Buch" ("Account 4"). A few minutes later, Instagram account #####37627 was created using the name "Jack_Back" and username "Jackb696" ("Account 5"). Based on my review of Account 4 and Account 5, I determined those accounts were created by the same user who created Facebook account #####73211 ("Account 6"). Account 6 was created on April 20, 2008, using the name "Oren Dor." Based on publicly available information from the BrandTotal website, I know Oren Dor to be BrandTotal's Chief Product Officer. Account 4 was disabled on October 16, 2020. Account 5 was disabled on October 18, 2020. Account 6 was disabled on September 30, 2020.

I declare under penalty of perjury that the foregoing is true and correct. Executed at Mountain View, CA, on the 21st day of October, 2020.



Sanchit Karve